WEST Search History

DATE: Wednesday, June 25, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L9	L8 and @pd>=19990327	34	L9
L8	((black$ adj box$) same (encrypt$ or decrypt$)) and ((black$ adj box$) same ((private$ or public$) with key$))	39	L8
L7	((black$ adj box$) same (encrypt$ or decrypt$)) and ((black$ adj box$) same ((private$ or public$) with key$)) and @pd<=19990327	5	L7
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L6	L5 and rights	12	L6
L5	L3 and ((black$ adj box$) same ((private$ or public$) with key$))	16	L5
L4	L3 and l1	1	L4
L3	((black$ adj box$) same (encrypt$ or decrypt$)) and @ad<=19990327	55	L3
L2	L1 and (encrypt$ or decrypt$)	3	L2
L1	((black$ adj box$) with server) and @ad<=19990327	55	L1

END OF SEARCH HISTORY

considered

```
S ((BLACK (W) BOX) (5N) SERVER) AND (ENCRYPT$ OR DECRYPT?) AND PD<=990327

Your SELECT statement is:
   S ((BLACK (W) BOX) (5N) SERVER) AND (ENCRYPT$ OR DECRYPT?) AND
PD<=990327

           Items   File
           -----   ----
Processing
       Examined  50 files
       Examined 100 files
       Examined 150 files
       Examined 200 files
       Examined 250 files
       Examined 300 files
       Examined 350 files

   No files have one or more items; file list includes 361 files.
   One or more terms were invalid in 198 files.

?
```

considered

```
S ((BLACK (W) BOX (W) SERVER) (S) (ENCRYPT? OR DECRYPT?)) AND PD<=990327
```

```
Your SELECT statement is:
   S ((BLACK (W) BOX (W) SERVER) (S) (ENCRYPT? OR DECRYPT?)) AND PD<=990327

          Items   File
          -----   ----
      Examined  50 files
      Examined 100 files
      Examined 150 files
      Examined 200 files
      Examined 250 files
      Examined 300 files
      Examined 350 files

   No files have one or more items; file list includes 361 files.
   One or more terms were invalid in 198 files.

?
```

considered

```
S (("BLACK-BOX" (W) SERVER) (S) (ENCRYPT? OR DECRYPT?)) AND PD<=990327

Your SELECT statement is:
   S (("BLACK-BOX" (W) SERVER) (S) (ENCRYPT? OR DECRYPT?)) AND PD<=990327

          Items   File
          -----   ----
      Examined  50 files
      Examined 100 files
      Examined 150 files
      Examined 200 files
      Examined 250 files
      Examined 300 files
      Examined 350 files

   No files have one or more items; file list includes 361 files.
   One or more terms were invalid in 198 files.

?
```

Generate Collection | Print

L7: Entry 1 of 5 File: USPT Oct 6, 1998

US-PAT-NO: 5818934
DOCUMENT-IDENTIFIER: US 5818934 A

TITLE: Method and apparatus for providing a cryptographically secure interface between the decryption engine and the system decoder of a digital television receiver

DATE-ISSUED: October 6, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Cuccia; David William	Hopewell Junction	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Phillips Electronics North America Corporation	New York	NY			02

APPL-NO: 08/ 768489 [PALM]
DATE FILED: December 18, 1996

INT-CL: [06] H04 K 1/02, H04 K 1/04, H04 K 1/06, H04 N 7/167

US-CL-ISSUED: 380/9; 380/10, 380/35, 380/36, 380/37
US-CL-CURRENT: 380/216; 380/228, 380/35, 380/36, 380/37, 713/192

FIELD-OF-SEARCH: 380/9, 380/10, 380/35-37

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4944006	July 1990	Citta et al.	380/20
☐	5535275	July 1996	Sugisaki et al.	380/10
☐	5689569	November 1997	Peyret	380/49

ART-UNIT: 362

PRIMARY-EXAMINER: Tarcza; Thomas H.

ASSISTANT-EXAMINER: Sayadian; Hrayr A.

ATTY-AGENT-FIRM: Gathman; Laurie E.

ABSTRACT:

A method for providing a secure interface between a decryption engine and a system decoder of a digital receiver, e.g., an MPEG-2 digital television receiver. The system decoder receives an encrypted bitstream and produces a cipher text bitstream which is supplied to the decryption engine via a first parallel data bus which includes a plurality N of parallel bit lines corresponding to respective N bits of the cipher text bitstream. The decryption engine decrypts the cipher text bitstream and produces a plain text bitstream which is supplied to the system decoder via a second parallel data bus which includes a plurality N of parallel bit lines corresponding to respective N bits of the plain text bitstream. The method includes the steps of scrambling the bit order of the N bits of the cipher text bitstream on the respective N bit lines of the first data bus, to thereby produce a scrambled cipher text bitstream N-bits wide, descrambling the bit order of the N bits of the scrambled cipher text bitstream, to thereby produce a descrambled cipher text bitstream which is the same as the original cipher text bitstream, employing the decryption engine to decrypt the descrambled cipher text bitstream, to thereby produce the plain text bitstream, scrambling the bit order of the N bits of the plain text bitstream on the respective N bit lines of the second data bus, to thereby produce a scrambled plain text bitstream N-bits wide, and descrambling the bit order of the N bits of the scrambled plain text bitstream, to thereby produce a descrambled plain text bitstream which is the same as the original plain text bitstream. A digital receiver which implements this method is also disclosed.

50 Claims, 1 Drawing figures

Generate Collection | Print

L7: Entry 4 of 5 File: USPT Apr 30, 1996

US-PAT-NO: 5513260
DOCUMENT-IDENTIFIER: US 5513260 A

TITLE: Method and apparatus for copy protection for various recording media

DATE-ISSUED: April 30, 1996

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ryan; John O.	Cupertino	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Macrovision Corporation	Sunnyvale	CA			02

APPL-NO: 08/ 267635 [PALM]
DATE FILED: June 29, 1994

INT-CL: [06] G11 B 23/28, H04 L 9/30

US-CL-ISSUED: 380/3; 380/5, 380/22, 369/44.33
US-CL-CURRENT: 380/200; 360/60, 369/44.33, 369/47.12, 369/53.21, 380/201, 380/202, 380/22, 713/176

FIELD-OF-SEARCH: 380/3, 380/4, 380/5, 380/23, 380/25, 369/44.26, 369/44.33

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4670857	June 1987	Rackman	380/4
☐	4785361	November 1988	Brotby	380/4 X
☐	4866769	September 1989	Karp	380/4
☐	4891504	January 1990	Gupta	360/60
☐	5159633	October 1992	Nakamura	380/30
☐	5379433	January 1995	Yamagishi	380/4 X
☐	5412718	May 1995	Narasimhalu et al.	380/4
☐	5418852	May 1995	Itami et al.	380/4

ART-UNIT: 222

PRIMARY-EXAMINER: Bar[redacted], Jr.; Gilberto

ATTY-AGENT-FIRM: Brill; Gerow D.

ABSTRACT:

A method and apparatus for copyright protection for various recording media such as compact discs (CDs) uses a combination of symmetrical and asymmetrical data encryption to permit the player to handle either copy-protected or non-copy-protected media, in a manner that is extremely difficult to compromise. Coupled with the combination of encrypting methods, an Authenticating Signature is recorded on the media only when copy-protection is required. The nature of this Authenticating Signature is such that it will not be transferred to illicit copies made on CD recorders. When either an original protected or an original non-protected disk is played, the presence or absence of the Authenticating Signature causes the player to correctly decrypt the program data. All original CDs therefore play normally. When a copy of a non-protected CD is played, the absence of the Authenticating Signature also causes the player to correctly decrypt the program data. However, when a copy of a protected CD is played, the absence of the Authenticating Signature causes the player to generate false data which prohibits the disk from playing normally.

25 Claims, 2 Drawing figures

L7: Entry 4 of 5 File: USPT Apr 30, 1996

DOCUMENT-IDENTIFIER: US 5513260 A
TITLE: Method and apparatus for copy protection for various recording media

DATE_ISSUED (1):
19960430

Detailed Description Text (3):
As mentioned earlier, it is desirable to be able to offer copy-protection to copyright holders on a program-by-program basis and to receive a per-program fee or a per-disk fee in return. This is accomplished in the Programmable Conditional Play System using a combination of symmetrical and asymmetrical (also known as public-key) data encryption to permit the CD-player to handle either copy protected or non-copy-protected disks in a manner that is extremely difficult or prohibitively expensive and time consuming to compromise, using black boxes.

Detailed Description Text (22):
1. Convert the doubly encrypted program data recorded on all copy-protected disks to the singly encrypted format required by CD-players when the Authenticating Signature is missing. To do this, the pirate must obtain the Secret Key P used in the disk mastering process, which as explained earlier can be closely guarded within a sealed, booby trapped unit located at the disk mastering plant. The pirate can readily access the doubly encrypted off disk data inside a CD-player. He may also access the partially decrypted and fully decrypted (clear) program data, along with keys K and Q, inside a CD-player. However, the essence of the asymmetrical encryption method is such that a pirate still does not have enough information to deduce the secret key P needed to generate the required singly encrypted program data. This compound encryption scheme thus permits selective protection of programs and is immune to black box attack.

End of Result Set

Generate Collection | Print

L7: Entry 5 of 5 File: USPT Jun 5, 1984

US-PAT-NO: 4453074
DOCUMENT-IDENTIFIER: US 4453074 A

TITLE: Protection system for intelligent cards

DATE-ISSUED: June 5, 1984

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Weinstein; Stephen B.	Summit	NJ		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
American Express Company	New York	NY			02

APPL-NO: 06/ 312705 [PALM]
DATE FILED: October 19, 1981

INT-CL: [03] G06K 5/00

US-CL-ISSUED: 235/380; 235/381, 235/382
US-CL-CURRENT: 705/66; 235/380, 235/381, 235/382, 380/281, 380/30, 713/173, 902/26, 902/5

FIELD-OF-SEARCH: 235/379, 235/380, 235/381, 235/382, 178/22.08, 340/825.32

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4288659	September 1981	Atalla	235/380 X

ART-UNIT: 214

PRIMARY-EXAMINER: Pitts; Harold I.

ATTY-AGENT-FIRM: Gottlieb, Rackman and Reisman

ABSTRACT:

There is disclosed a protection system for intelligent cards. Each card has stored in it a code which is the encryption of a concatenation of a user secret password and a common reference text. The encryption is derived by an initialization terminal which uses the private key associated with the public key of a public-key cryptosystem key pair. Each transaction terminal with which a card is used decrypts

the stored code in accordance with the public key. A transaction is effected only if the stored code decrypts into the user password which is inputted on a keyboard and the common reference text.

19 Claims, 7 Drawing figures

End of Result Set

Generate Collection | Print

L7: Entry 5 of 5 File: USPT Jun 5, 1984

DOCUMENT-IDENTIFIER: US 4453074 A
TITLE: Protection system for intelligent cards

DATE ISSUED (1):
19840605

Detailed Description Text (18):
Just as a sophisticated forger is assumed to know the transformation F of FIG. 3A, he is assumed to know the public key E of FIG. 3B since there will be many transaction terminals in the field and it is a relatively simple matter to learn the public key. Suppose that the forger tries to do with the system of FIG. 3B something comparable to what he can do with the system of FIG. 3A, namely, to select an arbitrary identification number, to decrypt it using the known public key E, and to then use the decrypted results in creating a "black box" or forged card which can fool a transaction terminal. A terminal can be "fooled" only if the decryption results in a password and the message text AMERICAN EXPRESS. Should an arbitrarily selected identification number, after decryption with the public key E, indeed result in the message text AMERICAN EXPRESS in the proper place (e.g., at the end) and some additional arbitrary combination of letters and numerals, this latter combination would be the password which the forger could then use in his "black box" or to input on the keyboard. But the arbitrary selection of an identification number would have an infinitesimal probability of its decryption consisting of the predetermined message text in the right place, together with some arbitrary combination of characters. Thus knowing the public key E is not sufficient to allow a forger to select an identification number (the combination of a password and the message text AMERICAN EXPRESS, as encrypted by the secret key of the issuer) which will effect a transaction. The only way that an identification number can be selected which will decrypt with the public key into a password part and a predetermined message text part is if the private key is used in the encryption process, and the forger has no way of knowing the private key.

Detailed Description Text (19):
It is essential that the result of the decryption consist of both a password part and a predetermined reference text part. Were the encryption stored on the card to consist of a password only, the forger could select an arbitrary identification number, decrypt it with the public key E, and use the result as his password; storage of the arbitrarily selected identification number in the "black box" to be used with a terminal as the encrypted code on a card would always result in a successful comparison were the forger to input the password derived by using the public key E. Similarly, were the code on the card to consist of nothing more than the message text AMERICAN EXPRESS encrypted with the private key D, all the forger would have to do is to determine the same encryption which is stored on every card and to use it in his "black box". Decryption in any terminal with the public key E would necessarily result in the reference text AMERICAN EXPRESS. What is necessary for security is to store in a card the code which is an encryption, created with the private key D, of a combination of a password and a predetermined reference text. There is no way--even with knowledge of the public key E--that a forger can select an arbitrary identification number, or encryption to be stored on a card, which will decrypt into some arbitrary password together with the predetermined reference text in the correct position in the concatenated strings.

End of Result Set

Generate Collection | Print

L6: Entry 12 of 12 File: USPT Jun 5, 1984

DOCUMENT-IDENTIFIER: US 4453074 A
TITLE: Protection system for intelligent cards

Application Filing Date (1):
19811019

Brief Summary Text (21):
The security of the present invention is precisely in its storage in the card of the encryption, using the issuer's private key, of a combination of a password unique to the user and a common reference text. It will no longer do the forger any good to start out with an arbitrary code. That arbitrary code (which the forger's unauthorized card would furnish to the terminal) must decrypt into two strings, one of which is the predetermined reference text AMERICAN EXPRESS. In accordance with the principles of public-key encryption, and assuming judiciously selected string lengths, the probability is infinitesimal of a forger selecting a random code which, when decrypted with the public key, has a predetermined substring in it. Were this to happen, the forger could look at the decrypted password/reference text combination, and see which password he would thereafter have to input to a terminal in order to effect both matches when his forged card inputs the random code which was tried in the first place. But the probability of an arbitrarily selected code being decrypted into a string, part of which is a predetermined reference text, is so negligible that the system is highly secure (certainly secure enough for commercial transactions.) The system is viable so long as the forger cannot determine the private key D which is the complement of the public key E stored in every transaction terminal. Without the private key, there is no technique of acceptable computational complexity which will specify a code which, when decrypted with the public key, will result in a string having a predetermined reference text as a substring. Even were some arbitrarily selected code decrypted into a string which would include as a part thereof the predetermined reference text AMERICAN EXPRESS, the predetermined reference text would have to occur in the right position in the overall decrypted password/reference text combination, and the probability of this happening is even more remote than that of guessing a code which will decrypt into an overall string which has the reference text AMERICAN EXPRESS in some arbitrary position.

Detailed Description Text (18):
Just as a sophisticated forger is assumed to know the transformation F of FIG. 3A, he is assumed to know the public key E of FIG. 3B since there will be many transaction terminals in the field and it is a relatively simple matter to learn the public key. Suppose that the forger tries to do with the system of FIG. 3B something comparable to what he can do with the system of FIG. 3A, namely, to select an arbitrary identification number, to decrypt it using the known public key E, and to then use the decrypted results in creating a "black box" or forged card which can fool a transaction terminal. A terminal can be "fooled" only if the decryption results in a password and the message text AMERICAN EXPRESS. Should an arbitrarily selected identification number, after decryption with the public key E, indeed result in the message text AMERICAN EXPRESS in the proper place (e.g., at the end) and some additional arbitrary combination of letters and numerals, this latter combination would be the password which the forger could then use in his "black box" or to input on the keyboard. But the arbitrary selection of an identification number would have an infinitesimal probability of its decryption consisting of the predetermined message text in the right place, together with some arbitrary combination of characters. Thus knowing the public key E is not sufficient to allow a forger to select an identification number (the combination of a password and the

message text AMERICAN EXPRESS, as encrypted by the secret key of the issuer) which will effect a transaction. The only way that an identification number can be selected which will decrypt with the public key into a password part and a predetermined message text part is if the private key is used in the encryption process, and the forger has no way of knowing the private key.

Detailed Description Text (19):
It is essential that the result of the decryption consist of both a password part and a predetermined reference text part. Were the encryption stored on the card to consist of a password only, the forger could select an arbitrary identification number, decrypt it with the public key E, and use the result as his password; storage of the arbitrarily selected identification number in the "black box" to be used with a terminal as the encrypted code on a card would always result in a successful comparison were the forger to input the password derived by using the public key E. Similarly, were the code on the card to consist of nothing more than the message text AMERICAN EXPRESS encrypted with the private key D, all the forger would have to do is to determine the same encryption which is stored on every card and to use it in his "black box". Decryption in any terminal with the public key E would necessarily result in the reference text AMERICAN EXPRESS. What is necessary for security is to store in a card the code which is an encryption, created with the private key D, of a combination of a password and a predetermined reference text. There is no way--even with knowledge of the public key E--that a forger can select an arbitrary identification number, or encryption to be stored on a card, which will decrypt into some arbitrary password together with the predetermined reference text in the correct position in the concatenated strings.

Detailed Description Text (34):
FIG. 7 depicts the flow chart which characterizes operation of a transaction terminal. The first step involves inputting of the password by the card owner. Because card owners often input their respective passwords incorrectly, a card owner is given four attempts to key in his password in the correct manner. A count j is set equal to one and the terminal then requests, via the display, that the user input his password. The terminal then transmits the inputted password to the card where it is compared with the stored user password. The comparison is best performed on the card, rather than in the terminal, for security purposes so that there is no way for someone who has tampered with the terminal to gain access to the user password. If the inputted password does not agree with that on the card, count j is incremented, and it is then compared with a maximum count of five. If j equals five, it is an indication that a user has attempted to input a correct password four times and has failed. It is therefore assumed that he is not the card owner, and the whole process is aborted as shown in the flow chart of FIG. 7. On the other hand, if he has inadvertently entered the wrong password, he is given another three chances to get it right. As long as the correct password of the card user is entered correctly within four attempts, the processing continues.

L9: Entry 33 of 34 File: DWPI Jul 19, 2001

DERWENT-ACC-NO: 2001-496746
DERWENT-WEEK: 200154

TITLE: Digital rights management system operating on computing device when user requests an encrypted digital content to be rendered by the computer

INVENTOR: GANESAN, K; LIU, D ; PEINADO, M

PATENT-ASSIGNEE: MICROSOFT CORP (MICT)

PRIORITY-DATA: 2000US-0526290 (March 15, 2000), 2000US-176425P (January 14, 2000)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 200152021 A1	July 19, 2001	E	126	G06F001/00
AU 200069281 A	July 24, 2001		000	G06F001/00

DESIGNATED-STATES: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
WO 200152021A1	August 22, 2000	2000WO-US23108	
AU 200069281A	August 22, 2000	2000AU-0069281	
AU 200069281A		WO 200152021	Based on

INT-CL (IPC): G06 F 1/00

RELATED-ACC-NO: 2001-522158;2001-522159 ;2001-596328 ;2001-596397

ABSTRACTED-PUB-NO: WO 200152021A
BASIC-ABSTRACT:

NOVELTY - Uses a black box (30) in the digital rights management (DRM) system for performing decryption and encryption functions. The black box contains identifier of computing device (14) and is tied to the computing device.

DETAILED DESCRIPTION - The black box also contains at least one black box public key. The DRM system also contains digital license (16) corresponding to the digital content. The licence includes a decryption key (KD) for decrypting the encrypted digital content. The decryption key is encrypted according to a black box public key of the black box. The licence is tied to the black box, and the computing device. AN INDEPENDENT CLAIM is made for a method of operating DRM system when user requests that computer renders an encrypted digital content.

USE - For enforcing rights in a digital content allowing access to encrypted digital content only in accordance with parameters specified by licence rights acquired by user.

ADVANTAGE - Enforceme[redacted]rights and method enforce righ[redacted]in protected (secure) digital content available on a medium such as the Internet, an optical disk, etc.

DESCRIPTION OF DRAWING(S) - Drawing is a block diagram showing an enforcement architecture in accordance with an embodiment of the present invention.

Computing device 14

Digital licence 16

Black box 30

Decryption key. KD

ABSTRACTED-PUB-NO: WO 200152021A
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.1/22

DERWENT-CLASS: T01
EPI-CODES: T01-C01A; T01-D01; T01-H01B1; T01-H01C2; T01-H07C5E; T01-J12C; T01-J20B2A;

End of Result Set

Generate Collection | Print

L9: Entry 34 of 34 File: DWPI Oct 5, 2000

DERWENT-ACC-NO: 2001-191170
DERWENT-WEEK: 200242

TITLE: Black box obtaining method of digital rights management system in personal computer, by determining unique black box having public and private key pair to digital rights management system from black box server

INVENTOR: ENGLAND, P; PEINADO, M ; VENKATESAN, R

PATENT-ASSIGNEE: MICROSOFT CORP (MICT)

PRIORITY-DATA: 2000US-0482840 (January 13, 2000), 1999US-126614P (March 27, 1999), 1999US-0290363 (April 12, 1999)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 200057684 A2	October 5, 2000	E	087	G06F007/00
AU 200033809 A	October 16, 2000		000	G06F007/00

DESIGNATED-STATES: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
WO 200057684A2	February 25, 2000	2000WO-US04946	
AU 200033809A	February 25, 2000	2000AU-0033809	
AU 200033809A		WO 200057684	Based on

INT-CL (IPC): G06 E 7/00

RELATED-ACC-NO: 2000-611744;2000-647267 ;2000-647268 ;2001-090815 ;2001-210824 ;2001-210825 ;2002-279866 ;2002-350656 ;2002-392575

ABSTRACTED-PUB-NO: WO 200057684A
BASIC-ABSTRACT:

NOVELTY - A unique black box having a public and private key pair is generated by a black box server, in response to a request from digital rights management system (DRM). The black box is then delivered to the DRM which then installs the black box.

DETAILED DESCRIPTION - The DRM requests for black box to the black box server via Internet connection when the previously installed black box is not current or non-unique. The black box is generated by the black server and delivered to the DRAM along with an identifying indicating currency, version number, digital certificate. A portion of the private key of the generated black box is encrypted according to software code associated with generated black box. An INDEPENDENT CLAIM is also included for black box obtaining program.

USE - For enforcing rights in digital content such as digital audio, digital text, digital multimedia in personal computer.

ADVANTAGE - Prevents user of the computing device from making copy of digital content, except allowed by the content owner.

DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram illustrating the steps performed in connection with DRM system.

ABSTRACTED-PUB-NO: WO 200057684A
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.9/12

DERWENT-CLASS: T01 T03 W04
EPI-CODES: T01-D01; T01-H07C3D; T01-H07C5S; T01-J12C; T03-P07; W04-F01L; W04-G01L;

Search Results - Record(s) 11 through 20 of 34 returned.

☐ 11. Document ID: US 20020013772 A1

L9: Entry 11 of 34 File: PGPB Jan 31, 2002

PGPUB-DOCUMENT-NUMBER: 20020013772
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020013772 A1

TITLE: Binding a digital license to a portable device or the like in a digital rights management (DRM) system and checking out / checking in the digital license to / from the portable device or the like

PUBLICATION-DATE: January 31, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Peinado, Marcus	Bellevue	WA	US	

US-CL-CURRENT: 705/51; 713/200

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

☐ 12. Document ID: US 20020012432 A1

L9: Entry 12 of 34 File: PGPB Jan 31, 2002

PGPUB-DOCUMENT-NUMBER: 20020012432
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020012432 A1

TITLE: Secure video card in computing device having digital rights management (DRM) system

PUBLICATION-DATE: January 31, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
England, Paul	Bellevue	WA	US	
Peinado, Marcus	Bellevue	WA	US	
Sankaranarayan, Mukund	Issaquah	WA	US	

US-CL-CURRENT: 380/231; 705/51, 705/59

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

☐ 13. Document ID: US 20020007456 A1

L9: Entry 13 of 34 File: PGPB Jan 17, 2002

PGPUB-DOCUMENT-NUMBER: 20020007456
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020007456 A1

TITLE: Secure processor architecture for use with a digital rights management (DRM) system on a computing device

PUBLICATION-DATE: January 17, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Peinado, Marcus	Bellevue	WA	US	
England, Paul	Bellevue	WA	US	

US-CL-CURRENT: 713/164

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 14. Document ID: US 20020006204 A1

L9: Entry 14 of 34 File: PGPB Jan 17, 2002

PGPUB-DOCUMENT-NUMBER: 20020006204
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020006204 A1

TITLE: Protecting decrypted compressed content and decrypted decompressed content at a digital rights management client

PUBLICATION-DATE: January 17, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
England, Paul	Bellevue	WA	US	
Peinado, Marcus	Bellevue	WA	US	
Sankaranarayan, Mukund	Issaquah	WA	US	

US-CL-CURRENT: 380/269; 705/51

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 15. Document ID: US 20010033655 A1

L9: Entry 15 of 34 File: PGPB Oct 25, 2001

PGPUB-DOCUMENT-NUMBER: 20010033655
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20010033655 A1

TITLE: Timing attack resistant cryptographic system

PUBLICATION-DATE: October 25, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Vadekar, Ashok	Rockwood		CA	
Lambert, Robert J.	Cambridge		CA	

US-CL-CURRENT: 380/28; 708/492, 713/174

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 16. Document ID: US 20010000709 A1

L9: Entry 16 of 34 File: PGPB May 3, 2001

PGPUB-DOCUMENT-NUMBER: 20010000709
PGPUB-FILING-TYPE: new-utility
DOCUMENT-IDENTIFIER: US 20010000709 A1

TITLE: Software distribution system and software utilization scheme for improving security and user convenience

PUBLICATION-DATE: May 3, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Takahashi, Toshinari	Tokyo		JP	
Nogami, Hiroyasu	Kanagawa		JP	

US-CL-CURRENT: 380/277; 705/51

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 17. Document ID: US 6427140 B1

L9: Entry 17 of 34 File: USPT Jul 30, 2002

US-PAT-NO: 6427140
DOCUMENT-IDENTIFIER: US 6427140 B1
**** See image for Certificate of Correction ****

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 18. Document ID: US 6389402 B1

L9: Entry 18 of 34 File: USPT May 14, 2002

US-PAT-NO: 6389402
DOCUMENT-IDENTIFIER: US 6389402 B1

**** See image for Certificate of Correction ****

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 19. Document ID: US 6363488 B1

L9: Entry 19 of 34 File: USPT Mar 26, 2002

US-PAT-NO: 6363488
DOCUMENT-IDENTIFIER: US 6363488 B1
**** See image for Certificate of Correction ****

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 20. Document ID: US 6332025 B1

L9: Entry 20 of 34 File: USPT Dec 18, 2001

US-PAT-NO: 6332025
DOCUMENT-IDENTIFIER: US 6332025 B1

TITLE: Software distribution system and software utilization scheme for improving security and user convenience

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

Generate Collection | Print

Terms	Documents
L8 and @pd>=19990327	34

Display Format: - Change Format

Previous Page Next Page

Search Results - Record(s) 21 through 30 of 34 returned.

☐ 21. Document ID: US 6253193 B1

L9: Entry 21 of 34 File: USPT Jun 26, 2001

US-PAT-NO: 6253193
DOCUMENT-IDENTIFIER: US 6253193 B1
**** See image for Certificate of Correction ****

TITLE: Systems and methods for the secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw. Desc | Image

☐ 22. Document ID: US 6237786 B1

L9: Entry 22 of 34 File: USPT May 29, 2001

US-PAT-NO: 6237786
DOCUMENT-IDENTIFIER: US 6237786 B1

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw. Desc | Image

☐ 23. Document ID: US 6237098 B1

L9: Entry 23 of 34 File: USPT May 22, 2001

US-PAT-NO: 6237098
DOCUMENT-IDENTIFIER: US 6237098 B1

TITLE: System for protecting weight verification device private key

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw. Desc | Image

☐ 24. Document ID: US 6195432 B1

L9: Entry 24 of 34 File: USPT Feb 27, 2001

US-PAT-NO: 6195432
DOCUMENT-IDENTIFIER: US 6195432 B1

TITLE: Software distribution system and software utilization scheme for improving security and user convenience

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 25. Document ID: US 5991415 A

L9: Entry 25 of 34 File: USPT Nov 23, 1999

US-PAT-NO: 5991415
DOCUMENT-IDENTIFIER: US 5991415 A

TITLE: Method and apparatus for protecting public key schemes from timing and fault attacks

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 26. Document ID: US 5982891 A

L9: Entry 26 of 34 File: USPT Nov 9, 1999

US-PAT-NO: 5982891
DOCUMENT-IDENTIFIER: US 5982891 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 27. Document ID: US 5949882 A

L9: Entry 27 of 34 File: USPT Sep 7, 1999

US-PAT-NO: 5949882
DOCUMENT-IDENTIFIER: US 5949882 A

TITLE: Method and apparatus for allowing access to secured computer resources by utilzing a password and an external encryption algorithm

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 28. Document ID: US 5949876 A

L9: Entry 28 of 34 File: USPT Sep 7, 1999

US-PAT-NO: 5949876
DOCUMENT-IDENTIFIER: US 5949876 A
**** See image for Certificate of Correction ****

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 29. Document ID: US 5917912 A

L9: Entry 29 of 34 File: USPT Jun 29, 1999

US-PAT-NO: 5917912
DOCUMENT-IDENTIFIER: US 5917912 A

TITLE: System and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 30. Document ID: US 5915019 A

L9: Entry 30 of 34 File: USPT Jun 22, 1999

US-PAT-NO: 5915019
DOCUMENT-IDENTIFIER: US 5915019 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

Generate Collection | Print

Terms	Documents
L8 and @pd>=19990327	34

Display Format: - Change Format

Previous Page Next Page

Search Results - Record(s) 31 through 34 of 34 returned.

☐ 31. Document ID: US 5910987 A

L9: Entry 31 of 34 File: USPT Jun 8, 1999

US-PAT-NO: 5910987
DOCUMENT-IDENTIFIER: US 5910987 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw. Desc | Image

☐ 32. Document ID: US 5892900 A

L9: Entry 32 of 34 File: USPT Apr 6, 1999

US-PAT-NO: 5892900
DOCUMENT-IDENTIFIER: US 5892900 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw. Desc | Image

☐ 33. Document ID: WO 200152021 A1 AU 200069281 A

L9: Entry 33 of 34 File: DWPI Jul 19, 2001

DERWENT-ACC-NO: 2001-496746
DERWENT-WEEK: 200154

TITLE: Digital rights management system operating on computing device when user requests an encrypted digital content to be rendered by the computer

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw. Desc | Clip Img | Image

☐ 34. Document ID: WO 200057684 A2 AU 200033809 A

L9: Entry 34 of 34 File: DWPI Oct 5, 2000

DERWENT-ACC-NO: 2001-191170
DERWENT-WEEK: 200242

TITLE: Black box obtaining method of digital rights management system in personal computer, by determining unique black box having public and private key pair to digital rights management system from black box server

Generate Collection | Print

Terms	Documents
L8 and @pd>=19990327	34

Display Format: - Change Format

Previous Page Next Page

Search Results - Record(s) 1 through 10 of 12 returned.

☐ 1. Document ID: US 6253193 B1

L6: Entry 1 of 12 File: USPT Jun 26, 2001

US-PAT-NO: 6253193
DOCUMENT-IDENTIFIER: US 6253193 B1
**** See image for Certificate of Correction ****

TITLE: Systems and methods for the secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

☐ 2. Document ID: US 6195432 B1

L6: Entry 2 of 12 File: USPT Feb 27, 2001

US-PAT-NO: 6195432
DOCUMENT-IDENTIFIER: US 6195432 B1

TITLE: Software distribution system and software utilization scheme for improving security and user convenience

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

☐ 3. Document ID: US 5982891 A

L6: Entry 3 of 12 File: USPT Nov 9, 1999

US-PAT-NO: 5982891
DOCUMENT-IDENTIFIER: US 5982891 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw. Desc | Image

☐ 4. Document ID: US 5949876 A

L6: Entry 4 of 12 File: USPT Sep 7, 1999

US-PAT-NO: 5949876
DOCUMENT-IDENTIFIER: US 5949876 A

** See image for Certificate of Correction **

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 5. Document ID: US 5917912 A

L6: Entry 5 of 12 File: USPT Jun 29, 1999

US-PAT-NO: 5917912
DOCUMENT-IDENTIFIER: US 5917912 A

TITLE: System and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 6. Document ID: US 5915019 A

L6: Entry 6 of 12 File: USPT Jun 22, 1999

US-PAT-NO: 5915019
DOCUMENT-IDENTIFIER: US 5915019 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 7. Document ID: US 5910987 A

L6: Entry 7 of 12 File: USPT Jun 8, 1999

US-PAT-NO: 5910987
DOCUMENT-IDENTIFIER: US 5910987 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 8. Document ID: US 5892900 A

L6: Entry 8 of 12 File: USPT Apr 6, 1999

US-PAT-NO: 5892900
DOCUMENT-IDENTIFIER: US 5892900 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 9. Document ID: US 5754649 A

L6: Entry 9 of 12 File: USPT May 19, 1998

US-PAT-NO: 5754649
DOCUMENT-IDENTIFIER: US 5754649 A

TITLE: Video media security and tracking system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 10. Document ID: US 5754648 A

L6: Entry 10 of 12 File: USPT May 19, 1998

US-PAT-NO: 5754648
DOCUMENT-IDENTIFIER: US 5754648 A

TITLE: Video media security and tracking system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

Generate Collection | Print

Terms	Documents
L5 and rights	12

Display Format: TI | Change Format

Previous Page Next Page

L6: Entry 1 of 12 File: USPT Jun 26, 2001

US-PAT-NO: 6253193
DOCUMENT-IDENTIFIER: US 6253193 B1
**** See image for Certificate of Correction ****

TITLE: Systems and methods for the secure transaction management and electronic rights protection

DATE-ISSUED: June 26, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 705/57; 705/52

ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

72 Claims, 155 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 146

Generate Collection | Print

L6: Entry 2 of 12 File: USPT Feb 27, 2001

US-PAT-NO: 6195432
DOCUMENT-IDENTIFIER: US 6195432 B1

TITLE: Software distribution system and software utilization scheme for improving security and user convenience

DATE-ISSUED: February 27, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Takahashi; Toshinari	Tokyo			JP
Nogami; Hiroyasu	Kanagawa			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Kabushiki Kaisha Toshiba	Kawasaki			JP	03

APPL-NO: 08/ 814538 [PALM]
DATE FILED: March 10, 1997

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	8-053407	March 11, 1996

INT-CL: [07] H04 L 9/12

US-CL-ISSUED: 380/9; 380/278, 380/284
US-CL-CURRENT: 380/277; 380/278, 380/284

FIELD-OF-SEARCH: 380/25, 380/21, 380/278, 380/283, 380/284, 395/650

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	Re36310	September 1999	Bjerrum et al.	380/25
☐	4200770	April 1980	Hellman et al.	178/22
☐	4405829	September 1983	Rivest et al.	178/22.1
☐	5809145	September 1998	Silk et al.	380/25
☐	5812666	September 1998	Baker et al.	380/21

ART-UNIT: 277

PRIMARY-EXAMINER: Peeso; Thomas R.

ASSISTANT-EXAMINER: Jack; Todd

ATTY-AGENT-FIRM: Foley & Lardner

ABSTRACT:

A software distribution system and a software utilization scheme for effectively preventing an illegal copy or a software is difficult while improving a convenience of a user. At a user side, a shared key to be shared between a software provider and a user is stored, where the shared key has a guaranteed correspondence with an ID information regarding a payment of a software fee by the user. Then, a desired software is requested to the software provider, and the desired software is received in an encrypted form from the software provider. The desired software received from the software provider is then decrypted by using the shared key stored at the user side, and the desired software in a decrypted form is utilized at the user side.

20 Claims, 17 Drawing figures

DOCUMENT-IDENTIFIER: US 6195432 B1
TITLE: Software distribution system and software utilization scheme for improving security and user convenience

Application Filing Date (1):
19970310

Brief Summary Text (9):
As it has been quite difficult to resolve all these problems completely by means of the software alone, there has been a proposition of a system called super-distribution which presumes a use of some special hardware. Namely, this is a system which uses a hardware functioning a black box that outputs some output data in response to an entered input data, while a content of this hardware itself cannot be analyzed even by the owner of this hardware. For example, it is possible to realize a scheme in which the encrypted data cannot be decrypted unless this function of a black box is available, by means of the conventional cryptographic technique such as the public key cryptosystem.

Brief Summary Text (12):
In FIG. 1, the left side represents a store which is offering the software for sale and the right side represents a customer who is trying to purchase the software. These store and customer are connected by a computer network (which will be abbreviated hereafter as a network) such as a telephone line or Internet. Note here that functions on the store side and functions on the customer side are basically to be realized by means of softwares.

Brief Summary Text (20):
On the other hand, in a case of using a system which requires a complicated procedure such as an entry of a credit card number of a customer or a user ID or a password assigned to that customer in every occasion of the purchase, it is practically impossible to realize an elaborated charging scheme such as that for charging three yen for the tomorrow's weather forecast (as a low value service will be disused when a procedure is complicated). As a consequence, only expensive softwares could be distributed successfully and some software right owners could profit enormously while some other software right owners could not profit at all, so that the proper growth of the software distribution cannot be expected.

Detailed Description Text (12):
FIG. 2 shows a typical configuration of a software distribution system in this first embodiment. In FIG. 2, the left side represents a store which sells a software, while the right side represents a customer who purchases the software, and the store and the customer are connected through a network.

Detailed Description Text (58):
This core software unit 35 is the main portion of the computer program which cannot be operated completely in this form. Further functions can be added to this main portion by adding the encrypted software to this core software unit 35, in other words, even when the encrypted software is executed by a person who has no right to decrypt this encrypted software, not all the functions of the software can be realized.

Detailed Description Text (75):
Moreover, the shared key is a key for use in the execution of the software as well as a key for use in the purchase of the software, so that it is both difficult as well as risky to make the illegal copy of the software, and consequently it becomes

pointless to commit [redacted] illegal art so that the protec[redacted]n of the copyright owner's right can be realized easily.

Detailed Description Text (128):
In other words, even when this software is executed by a person who has no right to decrypt this passive function file 437, not all the functions of the software can be realized.

L6: Entry 9 of 12 File: USPT May 19, 1998

US-PAT-NO: 5754649
DOCUMENT-IDENTIFIER: US 5754649 A

TITLE: Video media security and tracking system

DATE-ISSUED: May 19, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ryan; John O.	Cupertino	CA		
Morrison; E. Fraser	Redwood City	CA		
Copeland; Gregory C.	San Jose	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Macrovision Corp.	Sunnyvale	CA			02

APPL-NO: 08/ 880203 [PALM]
DATE FILED: June 23, 1997

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATION This application is a continuation of application Ser. No. 475592, filed Jun. 6, 1995, now abandoned, which is a continuation of commonly invented application Ser. No. 08/440,194, filed May 12, 1995, entitled Video Media Security and Tracking System.

INT-CL: [06] H04 L 9/00, H04 K 1/00, G11 B 15/04, G11 B 19/04, G07 D 7/00

US-CL-ISSUED: 380/4; 380/21, 380/23, 380/25, 360/60, 340/825.31, 340/825.34
US-CL-CURRENT: 380/203; 340/5.74, 340/5.86, 360/60, 705/57

FIELD-OF-SEARCH: 380/4, 380/3, 380/5, 380/21, 380/23, 380/25, 360/33.1, 360/60, 360/132-135, 369/48, 369/58, 369/59, 340/825.31, 340/825.34

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE DATE	PATENTEE-NAME	US-CL
☐	4453074	June 1984	Weinstein	235/380
☐	4866769	September 1989	Karp	380/4
☐	4991208	February 1991	Walker et al.	380/20
☐	5111504	May 1992	Esserman et al.	380/21
☐	5267311	November 1993	Bakhoum	380/4
☐	5379433	January 1995	Yamagishi	395/725
☐	5392351	February 1995	Hasebe et al.	380/4
☐	5400319	March 1995	Fite et al.	369/275.5
☐	5400403	March 1995	Fahn et al.	380/21
☐	5426701	June 1995	Herman et al.	380/52
☐	5450489	September 1995	Ostrover et al.	380/3
☐	5457746	October 1995	Dolphin	380/4
☐	5461675	October 1995	Diehl et al.	380/3
☐	5509073	April 1996	Monnin	380/20
☐	5537473	July 1996	Saward	380/16
☐	5555304	September 1996	Hasebe et al.	380/4
☐	5563947	October 1996	Kikinis	380/4
☐	5596639	January 1997	Kikinis et al.	380/4

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
A393955	October 1990	EP	
89/10615	November 1989	WO	
PCT/US96/04027	March 1996	WO	

ART-UNIT: 222

PRIMARY-EXAMINER: Tarcza; Thomas H.

ASSISTANT-EXAMINER: Sayadian; Hrayr A.

ATTY-AGENT-FIRM: Brill; Gerow D.

ABSTRACT:

A video disc designed for providing security and tracking data in the rental video media market. Those new formats for video players and media allow for inclusion of security features which both allow tracking of rental of such media and prevent unauthorized rental thereof Each player includes a decision circuit which plays a particular optical disc only if a player identification number recorded on a special separate magnetic track on the optical disk is the same as the player identification stored in the player, and if a movie identification number optically read from the disc matches a movie identification number recorded on the special separate magnetic track. A corresponding apparatus is provided at the video rental store which, at the time of rental, records on a magnetic portion of the media in encrypted form the movie identification number and the number of the particular disc player for which that rental is intended. The authorization encryption uses the private key of a

public key system, th[redacted]public key and the modulus bein[redacted]pre-recorded on the optical portion of the disc.

2 Claims, 4 Drawing figures

L6: Entry 9 of 12 File: USPT May 19, 1998

DOCUMENT-IDENTIFIER: US 5754649 A
TITLE: Video media security and tracking system

Application Filing Date (1):
19970623

Brief Summary Text (5):
As is well known, typically video tape cassettes or video discs containing prerecorded material such as movies are commercialized as follows. The owner of the copyrighted material on the video cassette or disc, i.e. the movie studio ("rights owner"), arranges for duplication of the movie onto a large number of video tape cassettes or discs. The video tape cassettes and discs are then sold by the movie studio to owners of video rental stores who then rent each video tape cassette or disc out as many times as they can, depending on demand. However, the owner of the video rental store only pays for each video tape cassette or disc once, because he has purchased it outright from the movie studio. Thus the bulk of the profits due to rental of such material accrue to the video rental store owner rather than to the movie studio. This is because the so-called "first sale doctrine" prevents the seller (the movie studio) of the video tape cassettes or discs from exercising any degree of control over the downstream commercialization (e.g., rental) of its products. This is the case even though the video material is copyrighted.

Brief Summary Text (6):
It has been frustrating to the rights owners (movie studios, etc.) that they are not able to better control and/or profit from the rental market for their movies and other program material. Various methods have been proposed to allow the rights owners to overcome the first sale doctrine and acquire some degree of control over the rental of, for instance, VHS video tape cassettes.

Brief Summary Text (11):
It is to be understood that the video store owners interests in this regard are to a large extent the same as those of the rights owners. If a reliable system could be found to share rental revenues between the rights owners and the video store owners, then the rights owners would provide many more copies of each movie for rental to each store, hence increasing profits for both parties.

Brief Summary Text (15):
Implementation of the present security system requires that a significant proportion of the rights owners agree on the desirability of being able to better control commercial use of their copyrighted materials for the new formats, and as a consequence that the manufacturers of the players would be receptive to making compatible players in the expectation of increased support for their formats.

Brief Summary Text (17):
The next attribute is a high level of system security; the present system is believed to be impossible (or prohibitively expensive on a practical basis) for unscrupulous video rental store owners (or hackers in collusion with video rental store owners) to cheat on or to compromise. Thus in accordance with the invention the rights owners can be confident that they are properly recompensed for rental activity. In the event of any security breach, in accordance with the invention it is possible quickly and inexpensively to recover from the breach and minimize resulting losses. Also, in accordance with the invention, there is tracking system security, in that particular rights owners are assured that transaction data relating to their particular video material (movie titles) is not accessible by others.

Detailed Description Text (12):
This system provides the above described advantages. In terms of functionality, for transaction tracking information the electronic clock in the TTRD notes each disc's time and date of authorization and when it was returned to the rental store. Combined with the movie title and renter's player identification if desired, this is sufficient information to track rental activity. It is to be noted however that in certain embodiments of the invention the rental tracking features are not necessary and only the below-described security features are included. Thus in certain applications where the rights owner may for instance not require transaction information but merely wants security, the functionality of transaction tracking and the accompanying structures may be dispensed with.

Detailed Description Text (15):
In order to prevent illicit transactions, that is to prevent a hacker from designing a "black box" device to illicitly record authorization data on an authorization card, this data (the player and movie identification) is concatenated and encrypted and written on the authorization card (or on each disc) by the TTRD, using a public key encryption system. Such systems are well known. The following is a brief review of pertinent encryption methods.

Detailed Description Text (25):
A vital feature of a public key encryption system is that it is not possible to deduce what the encrypted data would be for a block of data which differs by as little as one bit from a block of data whose encrypted value is already known. In other words, knowing the encrypted data for an instruction to allow e.g. movie number 566 to play on a player with player ID 1289, would not allow a hacker to deduce what encrypted data would correspond to an instruction to allow movie number 567 to play on the identical player. Thus the most a hacker could do would be to note the code sequence which authorizes playing a particular movie for a particular player and later reuse that same code sequence with the same customer desiring to rent the same movie at a later time. Thus at most such hacking would obtain for the unscrupulous rental store owner one additional rental without having to pay the rights owner for that one particular rental. The effort required to do this seems to vastly outweigh any likely financial gain and hence it would not be done.

Detailed Description Text (26):
In terms of restricting access to transaction data, the system also uses in one embodiment a public key encryption system (not the same one as above in terms of the keys themselves) to report transactions. Thus each rights owner (e.g. movie studio) is assigned a unique private key/public key pair. Each TTRD stores the public key of each studio. Transaction data relating to a particular studio is encrypted within the TTRD prior to storage and transmission of same, using that studio's public key. Only the studio (or its agent) is provided with the corresponding private key needed to decrypt the transaction data.

Detailed Description Text (28):
The TTRD in either embodiment includes a port and loading mechanism such as those of a DVD player. The authorization card and the disc are ejected in a few seconds and the first part of the transaction is automatically recorded. When later on the renter returns the disc (or soon thereafter) the employee again inserts the disc in the TTRD and indicates the return transaction on its keyboard interface. The final part of the transaction, i.e. the time of disc return, is now recorded and the disc is again ejected and replaced on the store shelves. The authorization card is merely returned for later reuse. Transaction reporting to the rights owner or its agent is done automatically, for instance via modem and telephone lines, at a convenient time. Transaction reporting may also be done by other well known means. Thus the effort required of the video rental store employee is only slightly greater than that required in existing rental stores using point of sale terminals to store customer information and bar code readers to check out and check in video tape cassettes or discs.

Detailed Description Text (37):
The program identification in addition to being used for tracking also increases system security. That is, if there were no program identification, the only information recorded on the magnetic track of the disc would be the encrypted player number. Thus a hacker could breach the security of the system by reading the authorization card to obtain the code to authorize play, i.e. enable use of a particular player, by merely reading and recording the encrypted data pertaining to

that player number. [redacted]ere is no need in this case fo[redacted]he hacker to decrypt this number but he merely needs to record the appropriate encrypted data on the magnetic track of the disc without using the TTRD, i.e. bypassing the TTRD, and thus cheating the rights owner by not recording the particular rental transaction. Thus by providing a piece of information which is unique to each rental transaction (a program identification number) and given the use of a public key system, it is made impossible for a hacker to determine what the encoded data would be for a different movie for the same player, due to the nature of public key encryption systems.

L7: Entry 2 of 5 File: USPT May 19, 1998

US-PAT-NO: 5754649
DOCUMENT-IDENTIFIER: US 5754649 A

TITLE: Video media security and tracking system

DATE-ISSUED: May 19, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ryan; John O.	Cupertino	CA		
Morrison; E. Fraser	Redwood City	CA		
Copeland; Gregory C.	San Jose	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Macrovision Corp.	Sunnyvale	CA			02

APPL-NO: 08/ 880203 [PALM]
DATE FILED: June 23, 1997

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATION This application is a continuation of application Ser. No. 475592, filed Jun. 6, 1995, now abandoned, which is a continuation of commonly invented application Ser. No. 08/440,194, filed May 12, 1995, entitled Video Media Security and Tracking System.

INT-CL: [06] H04 L 9/00, H04 K 1/00, G11 B 15/04, G11 B 19/04, G07 D 7/00

US-CL-ISSUED: 380/4; 380/21, 380/23, 380/25, 360/60, 340/825.31, 340/825.34
US-CL-CURRENT: 380/203; 340/5.74, 340/5.86, 360/60, 705/57

FIELD-OF-SEARCH: 380/4, 380/3, 380/5, 380/21, 380/23, 380/25, 360/33.1, 360/60, 360/132-135, 369/48, 369/58, 369/59, 340/825.31, 340/825.34

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

	PAT-NO	ISSUE DATE	PATENTEE-NAME	US-CL
☐	4453074	June 1984	Weinstein	235/380
☐	4866769	September 1989	Karp	380/4
☐	4991208	February 1991	Walker et al.	380/20
☐	5111504	May 1992	Esserman et al.	380/21
☐	5267311	November 1993	Bakhoum	380/4
☐	5379433	January 1995	Yamagishi	395/725
☐	5392351	February 1995	Hasebe et al.	380/4
☐	5400319	March 1995	Fite et al.	369/275.5
☐	5400403	March 1995	Fahn et al.	380/21
☐	5426701	June 1995	Herman et al.	380/52
☐	5450489	September 1995	Ostrover et al.	380/3
☐	5457746	October 1995	Dolphin	380/4
☐	5461675	October 1995	Diehl et al.	380/3
☐	5509073	April 1996	Monnin	380/20
☐	5537473	July 1996	Saward	380/16
☐	5555304	September 1996	Hasebe et al.	380/4
☐	5563947	October 1996	Kikinis	380/4
☐	5596639	January 1997	Kikinis et al.	380/4

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
A393955	October 1990	EP	
89/10615	November 1989	WO	
PCT/US96/04027	March 1996	WO	

ART-UNIT: 222

PRIMARY-EXAMINER: Tarcza; Thomas H.

ASSISTANT-EXAMINER: Sayadian; Hrayr A.

ATTY-AGENT-FIRM: Brill; Gerow D.

ABSTRACT:

A video disc designed for providing security and tracking data in the rental video media market. Those new formats for video players and media allow for inclusion of security features which both allow tracking of rental of such media and prevent unauthorized rental thereof Each player includes a decision circuit which plays a particular optical disc only if a player identification number recorded on a special separate magnetic track on the optical disk is the same as the player identification stored in the player, and if a movie identification number optically read from the disc matches a movie identification number recorded on the special separate magnetic track. A corresponding apparatus is provided at the video rental store which, at the time of rental, records on a magnetic portion of the media in encrypted form the movie identification number and the number of the particular disc player for which that rental is intended. The authorization encryption uses the private key of a

public key system, the public key and the modulus being pre-recorded on the optical portion of the disc.

2 Claims, 4 Drawing figures

L7: Entry 2 of 5 File: USPT May 19, 1998

DOCUMENT-IDENTIFIER: US 5754649 A
TITLE: Video media security and tracking system

DATE ISSUED (1):
19980519

Detailed Description Text (15):
In order to prevent illicit transactions, that is to prevent a hacker from designing a "black box" device to illicitly record authorization data on an authorization card, this data (the player and movie identification) is concatenated and encrypted and written on the authorization card (or on each disc) by the TTRD, using a public key encryption system. Such systems are well known. The following is a brief review of pertinent encryption methods.

End of Result Set

Generate Collection | Print

L6: Entry 12 of 12 File: USPT Jun 5, 1984

US-PAT-NO: 4453074
DOCUMENT-IDENTIFIER: US 4453074 A

TITLE: Protection system for intelligent cards

DATE-ISSUED: June 5, 1984

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Weinstein; Stephen B.	Summit	NJ		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
American Express Company	New York	NY			02

APPL-NO: 06/ 312705 [PALM]
DATE FILED: October 19, 1981

INT-CL: [03] G06K 5/00

US-CL-ISSUED: 235/380; 235/381, 235/382
US-CL-CURRENT: 705/66; 235/380, 235/381, 235/382, 380/281, 380/30, 713/173, 902/26, 902/5

FIELD-OF-SEARCH: 235/379, 235/380, 235/381, 235/382, 178/22.08, 340/825.32

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4288659	September 1981	Atalla	235/380 X

ART-UNIT: 214

PRIMARY-EXAMINER: Pitts; Harold I.

ATTY-AGENT-FIRM: Gottlieb, Rackman and Reisman

ABSTRACT:

There is disclosed a protection system for intelligent cards. Each card has stored in it a code which is the encryption of a concatenation of a user secret password and a common reference text. The encryption is derived by an initialization terminal which uses the private key associated with the public key of a public-key cryptosystem key pair. Each transaction terminal with which a card is used decrypts

the stored code in accordance with the public key. A transaction is effected only if the stored code decrypts into the user password which is inputted on a keyboard and the common reference text.

19 Claims, 7 Drawing figures

Generate Collection | Print

L6: Entry 11 of 12 File: USPT Apr 30, 1996

US-PAT-NO: 5513260
DOCUMENT-IDENTIFIER: US 5513260 A

TITLE: Method and apparatus for copy protection for various recording media

DATE-ISSUED: April 30, 1996

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ryan; John O.	Cupertino	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Macrovision Corporation	Sunnyvale	CA			02

APPL-NO: 08/ 267635 [PALM]
DATE FILED: June 29, 1994

INT-CL: [06] G11 B 23/28, H04 L 9/30

US-CL-ISSUED: 380/3; 380/5, 380/22, 369/44.33
US-CL-CURRENT: 380/200; 360/60, 369/44.33, 369/47.12, 369/53.21, 380/201, 380/202, 380/22, 713/176

FIELD-OF-SEARCH: 380/3, 380/4, 380/5, 380/23, 380/25, 369/44.26, 369/44.33

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4670857	June 1987	Rackman	380/4
☐	4785361	November 1988	Brotby	380/4 X
☐	4866769	September 1989	Karp	380/4
☐	4891504	January 1990	Gupta	360/60
☐	5159633	October 1992	Nakamura	380/30
☐	5379433	January 1995	Yamagishi	380/4 X
☐	5412718	May 1995	Narasimhalu et al.	380/4
☐	5418852	May 1995	Itami et al.	380/4

ART-UNIT: 222

PRIMARY-EXAMINER: Barr[redacted], Jr.; Gilberto

ATTY-AGENT-FIRM: Brill; Gerow D.

ABSTRACT:

A method and apparatus for copyright protection for various recording media such as compact discs (CDs) uses a combination of symmetrical and asymmetrical data encryption to permit the player to handle either copy-protected or non-copy-protected media, in a manner that is extremely difficult to compromise. Coupled with the combination of encrypting methods, an Authenticating Signature is recorded on the media only when copy-protection is required. The nature of this Authenticating Signature is such that it will not be transferred to illicit copies made on CD recorders. When either an original protected or an original non-protected disk is played, the presence or absence of the Authenticating Signature causes the player to correctly decrypt the program data. All original CDs therefore play normally. When a copy of a non-protected CD is played, the absence of the Authenticating Signature also causes the player to correctly decrypt the program data. However, when a copy of a protected CD is played, the absence of the Authenticating Signature causes the player to generate false data which prohibits the disk from playing normally.

25 Claims, 2 Drawing figures

DOCUMENT-IDENTIFIER: US 5513260 A
TITLE: Method and apparatus for copy protection for various recording media

Application Filing Date (1):
19940629

Brief Summary Text (8):
For the foregoing reasons, there is a need for a copy-protection system for the compact disc medium that provides a high level of protection to software rights owners, that is immune to black boxes and that is not compromised by the refusal of a few hardware manufacturers to comply with the standard.

Detailed Description Text (2):
The present invention relates to a method and apparatus for copy-protecting various program distribution media, such as the compact disk medium. This invention is applicable to all disk media and the principles may be extended by one of ordinary skill in the art to other media such as magnetic tape. The invention offers a high level of protection to software rights owners, is immune to black boxes and will not be compromised by the refusal of a few hardware manufacturers to comply with the standard.

Detailed Description Text (3):
As mentioned earlier, it is desirable to be able to offer copy-protection to copyright holders on a program-by-program basis and to receive a per-program fee or a per-disk fee in return. This is accomplished in the Programmable Conditional Play System using a combination of symmetrical and asymmetrical (also known as public-key) data encryption to permit the CD-player to handle either copy protected or non-copy-protected disks in a manner that is extremely difficult or prohibitively expensive and time consuming to compromise, using black boxes.

Detailed Description Text (22):
1. Convert the doubly encrypted program data recorded on all copy-protected disks to the singly encrypted format required by CD-players when the Authenticating Signature is missing. To do this, the pirate must obtain the Secret Key P used in the disk mastering process, which as explained earlier can be closely guarded within a sealed, booby trapped unit located at the disk mastering plant. The pirate can readily access the doubly encrypted off disk data inside a CD-player. He may also access the partially decrypted and fully decrypted (clear) program data, along with keys K and Q, inside a CD-player. However, the essence of the asymmetrical encryption method is such that a pirate still does not have enough information to deduce the secret key P needed to generate the required singly encrypted program data. This compound encryption scheme thus permits selective protection of programs and is immune to black box attack.

DOCUMENT-IDENTIFIER: US 5940507 A
TITLE: Secure file archive through encryption key management

Abstract Text (1):
A information processing system providing archive/backup support with privacy assurances by encrypting data stored thereby. Data generated on a source system is encrypted, the key used thereby is separately encrypted, and both the encrypted data and encrypted key are transmitted to and maintained by a data repository system. The repository system receives only the encrypted data and key, while the source system retains the ability to recover the key and in turn, the data. The source system is therefore assured of privacy and integrity of the archived data by retaining access control yet is relieved of the physical management of the warehousing medium.

Application Filing Date (1):
19980128

Brief Summary Text (10):
The present invention addresses the problem of privacy for archived data by providing the source organization with control over the data without burdening the reliability of retrieval with the problems caused by sequential overwrite. An encryption function applied to the archived data renders it in a form unintelligible to unauthorized observers. Encryption involves arithmetic manipulations of the data using a specific value called a key, which renders the data in an unintelligible form. This key bears a specific mathematical relationship to the data and the encryption algorithm being used. Returning the data to the original form involves applying the corresponding inverse function to the encrypted form. Without the proper key, however, it is very difficult to determine the inverse, or decryption, function. The security provided by encryption rests on the premise that with a sufficiently large key, substantial computational resources are required to determine the original data. Encrypting a file with a particular key, and then encrypting the key itself using a master key, therefore, allows another party to physically maintain and store the data while the originator, or source, of the data retains access control. Additional security and authentication measures can also be taken, such as further encrypting the key or the data at the server with a server key, and the use of cipher block chaining to impose dependencies among a sequence of file blocks.

Brief Summary Text (11):
In accordance with the present invention, an archive server utilizes encryption techniques to maintain both security and integrity of stored data by maintaining a series of keys for each archived file, and encrypting both the archived file, and the key to which it corresponds. The archive server manages the encrypted files and the corresponding encrypted keys, while the source organization maintains only the master key required to recover the individual encrypted keys. Through this arrangement, the source organization maintains control and assurances over access to the archived data, while the archive server manages the physical storage medium and performs individual encrypted file manipulation requests at the behest of the client. The archive server maintains access only to the encrypted data files and encrypted keys, effectively managing these files and keys as abstract black-box entities, without the ability to examine and interpret the contents.

Brief Summary Text (12):
Three common transactions involving archived encrypted files are effected by the present invention. A source organization desiring to archive files periodically transfers files from its online repository, usually a fast access storage medium

such as a disk, to the archive server. To retrieve archived information, a retrieval transaction indicating a particular file occurs. Finally, when an item is to be deleted, a deletion instruction implicating a particular file is issued to the archive server.

Detailed Description Text (4):
An archive transaction for a file stored at the source system encompasses encryption of the file on the source system using a secondary key, encryption of the secondary key on the source system using a master key, and transmission of the encrypted file and the associated encrypted key to the archive server. Transmission is electronic via computer network, or in alternative embodiments by physical delivery of a suitable magnetic medium. The archive server then stores the encrypted file on magnetic tape or another medium of long term storage, and stores the encrypted key along with an index to the tape containing the encrypted file. The master key used to encrypt the secondary key is retained on the source system.

Detailed Description Text (5):
Referring to FIGS. 1 and 2, A file 10 to be archived is identified 100 within a fast access storage medium 12 of the source information system 8, and is sent to a cryptographic engine 14. The present embodiment incorporates a disk drive as the fast access storage medium, although an alternative embodiment could use other modes of digital fixation, such as CD-ROM. The cryptographic engine 14 may be an application within the same node or an independent CPU, and may invoke specialized encryption hardware, depending on the encryption method desired. Any of various known encryption methods could be employed.

Detailed Description Text (6):
A key generator 16 then generates a secondary key 18 as shown in step 102, and uses this key to encrypt the file 10 as shown in step 104 to produce an encrypted file 20, at step 106. The master encryption key 22 is then obtained in step 108 and used to encrypt the secondary key in 18, as shown at step 110, and produce an encrypted key 24, as indicated in step 112. Note that since the same master key is used to encrypt multiple secondary keys it need be generated only once and then reused for successive secondary keys. The encrypted file 20 and encrypted key 24 are then transmitted to the archive server at steps 116 and 118, respectively, while the master key 22 is retained at the source system 8 at step 114. Transmission may be accomplished via Internet 26, dialup connection 28, or in alternative embodiments, other means such as physical delivery of the storage medium. Encryption may be performed by any of various known methods, such as RSA, DES, and other permutations and may involve authentication and verification either through a trusted third party or mathematical methods. Such authentication and verification may involve cipher block chaining (CBC), to perform an XOR on all or part of a previous block and use the resultant value in encrypting a successive block, or checksums such as cyclic redundancy checks (CRC), MD4, and MD5, which accumulate all values in a particular block according to a mathematical formula to arrive at a value which is highly unlikely to be duplicated if data in the block is changed or lost.

Detailed Description Text (7):
Upon receipt of the encrypted file 20 and the encrypted key 24, the archive server 30 writes the encrypted file 32 to a magnetic tape 36, or other medium of long term storage which is inexpensive and which need not encompass real time access, via tape drive 34 at step 120. The encrypted key 38 is then written to a tape index disk file 40 at step 122, thereby associating the magnetic tape volume 36 with the encrypted file 32 and the encrypted key 38. In alternative embodiments, a further encryption operation may be performed at the archive server on the encrypted file 32 or the encrypted key 38 to add an additional layer of security.

Detailed Description Text (8):
Recovery of a file is accomplished by the archive server referencing the index to obtain the encrypted key and the volume of the encrypted file. The encrypted file is then retrieved from the volume, and both the encrypted file and encrypted key are transmitted back to the client. The client then recovers the file through the same two stage process used to encrypt. First, the secondary key must be recovered by decrypting the encrypted key with the master. Second, the original file may be recovered by decrypting the encrypted file with the secondary key.

Detailed Description Text (9):
Referring to FIGS. 1 and 3, for file recovery the archive server searches the tape index disk file 40 at step 200 to lookup the encrypted key 44 and the location of

the magnetic tape volume 36. The server then retrieves the encrypted key at step 202 and retrieves the encrypted file 42 from long term storage via tape drive 34, as shown in step 204. The encrypted file 48 and encrypted key 46 are then transmitted back to the source system 8 as indicated by steps 206 and 208, respectively.

Detailed Description Text (10):
Once received by the source system 8, the master key 22 is used to decrypt the encrypted key 46 at step 210 and recover the secondary key 18, as shown in step 212. The secondary key 18 is then used to decrypt the encrypted file 48 as shown in step 214 to produce the recovered file 50 which is identical to the original file 10, as indicated by step 216.

Detailed Description Text (11):
File deletion involves searching the tape index disk file 40, for the entry corresponding to the file 10 marked for deletion. Rather than retrieving the key and volume, however, the encrypted key 44 is deleted and the storage area in the tape index disk file 40 overwritten with zero values. This overwriting is required to avoid future access to the encrypted key 44 through use of a sector level disk access, as many file systems merely flag a deleted area as available, and data physically remains unaltered until a subsequent write needs the available space. Elimination of the encrypted key effectively precludes future access to the contents of the archived file stored on magnetic tape without requiring physical modification to the archive volume; only the encrypted key is deleted. Therefore, there is no compromise of the integrity of adjacent entities on the tape, and no extraneous versions of sensitive data.

Detailed Description Text (12):
Following overwrite of the encrypted key 44, the information in the encrypted file 32 remains secure. No modification of the magnetic tape volume 36 is required, as the encryption ensures that the information remains unintelligible.

Detailed Description Text (13):
Effectiveness of this method suggests that the encryption take place no more remotely than the limits of the source system organization's proprietary, or internal, network, as unprotected electronic transfers can also compromise the data. The dotted line 52 on FIG. 1 indicates the extent of unencrypted data and should represent no greater extent than the intranet of the originating entity.

Detailed Description Text (14):
Master key generation is significant because recovery of a key allows recovery of the file that the key represents. Consequently, control over access and deletion to archived files is dependent upon control over the corresponding secondary keys. Each key, however, must be unique to the file to which it corresponds, otherwise, exposure of a key to decrypt a particular file compromises that key for all other files which that key covers. If the source system is required to maintain a separate key for all archived encrypted files, however, there is merely a shift in storage medium, as the key to each encrypted file, rather than the file, must be still be maintained. Encrypting individual secondary keys allows the keys to be maintained as securely as the files. The source system maintains a single master key, or several master keys covering different groups of secondary keys. Control of the archived, encrypted files is then focused through a master key. The archiving entity retains a set of all encrypted files, and maintains a mapping to the corresponding encrypted keys for which the source organization holds the master key.

CLAIMS:

1. An electronic network for transferring data units among storage elements comprising:

a communications link;

a source information processing system at a first end of said communications link further comprising:

a master encryption key;

at least one secondary encryption key;

a first memory for storing data units and said master and said at least one

secondary encryption keys; and

an encryption engine for selectively encrypting said data units to produce encrypted data units using at least one of said secondary encryption keys, and for encrypting said at least one secondary encryption key with said master encryption key producing at least one encrypted key; and

an archive server information processing system having at least one archive server key at a second end of said communications link comprising a second memory and in communication with said source information processing system, said archive server information processing system for receiving and storing said encrypted data units and said encrypted keys in said second memory wherein said archive server key is used to further encrypt said encrypted keys.

6. The network as in claim 4 wherein said at least one encrypted key is stored in said first storage area within said second memory and said encrypted data units are stored in said second storage area within said second memory.

9. The network as in claim 1 wherein said source information processing system further comprises a computer and said encryption engine is implemented by said computer executing an encryption application having said master encryption key, said at least one secondary key, and said data units as inputs and said encrypted data units and said at least one encrypted key as outputs.

10. The network as in claim 1 wherein said source information processing system further comprises a computer and said encryption engine is implemented by a circuit in communication with said computer, said circuit having said master encryption key, said at least one secondary encryption key, and said data units as inputs and said encrypted data units and said at least one encrypted key as outputs.

12. The network as in claim 1 wherein said data units comprise subdivisions comprising a plurality of blocks and said encryption is applied to said blocks wherein input to said encryption includes values from said plurality of blocks and the results of at least one previous encrypted block.

13. An electronic network for transferring data units among storage elements comprising:

a communications link;

a source information processing system at a first end of said communications link further comprising:

a master encryption key;

at least one secondary encryption key;

a first memory for storing data units and said master and said at least one secondary encryption keys; and

an encryption engine for selectively encrypting said data units to produce encrypted data units using at least one of said secondary encryption keys, and for encrypting said at least one secondary encryption key with said master encryption key producing at least one encrypted key; and

an archive server information processing system having at least one archive server key at a second end of said communications link comprising a second memory and in communication with said source information processing system, said archive server information processing system for receiving and storing said encrypted data units and said encrypted keys in said second memory wherein said archive server key is used to further encrypt said encrypted data units.

14. A method for providing secure archive for data generated in a first memory within a source information processing system comprising the steps of:

identifying data for archive within said first memory;

obtaining a secondary encryption key;

encrypting said data with said secondary encryption key to produce encrypted data;

obtaining a master encryption key;

encrypting said secondary encryption key with said master encryption key to produce an encrypted key;

transmitting said encrypted data and encrypted key to an archive information system having a second memory;

writing said encrypted data and said encrypted key to said second memory; and

overwriting the portion of said second memory where said encrypted key is stored.

20. The method according to claim 14 wherein said data is subdivided into a plurality of blocks and input to said encrypting includes the results of at least one previous encrypting of said blocks.

21. A method for providing secure archive for data generated in a first memory within a source information processing system comprising the steps of:

identifying data for archive within said first memory;

obtaining a secondary encryption key;

encrypting said data with said secondary encryption key to produce encrypted data;

obtaining a master encryption key;

encrypting said secondary encryption key with said master encryption key to produce an encrypted key;

transmitting said encrypted data and encrypted key to an archive information system having a second memory and an archive server encryption key;

further encrypting said encrypted key with said archive server encryption key;

writing said encrypted data and said encrypted key to said second memory.

22. A method for providing secure archive for data generated in a first memory within a source information processing system comprising the steps of:

identifying data for archive within said first memory;

obtaining a secondary encryption key;

encrypting said data with said secondary encryption key to produce encrypted data;

obtaining a master encryption key;

encrypting said secondary encryption key with said master encryption key to produce an encrypted key;

transmitting said encrypted data and encrypted key to an archive information system having a second memory and an archive server encryption key;

further encrypting said encrypted data with said archive server encryption key;

writing said encrypted data and said encrypted key to said second memory.

23. A method for providing secure archive for data generated in a first memory within a source information processing system comprising the steps of:

identifying data for archive within said first memory;

obtaining a secondary encryption key;

encrypting said data with said secondary encryption key to produce encrypted data;

obtaining a master encryption key;

encrypting said secondary encryption key with said master encryption key to produce an encrypted key;

transmitting said encrypted data and encrypted key to an archive information system having a second memory and an archive server encryption key;

writing said encrypted data and said encrypted key to said second memory

retrieving said encrypted data and said encrypted key from said second memory of said archive information system;

decrypting said encrypted key with said archive server encryption key;

transmitting said encrypted data and said encrypted key from said archive information system to said source information processing system;

decrypting said encrypted key with said master encryption key to recover said secondary key; and

decrypting said encrypted data with said secondary key to recover said data.

24. A method for providing secure archive for data generated in a first memory within a source information processing system comprising the steps of:

identifying data for archive within said first memory;

obtaining a secondary encryption key;

encrypting said data with said secondary encryption key to produce encrypted data;

obtaining a master encryption key;

encrypting said secondary encryption key with said master encryption key to produce an encrypted key;

transmitting said encrypted data and encrypted key to an archive information system having a second memory and an archive server encryption key;

writing said encrypted data and said encrypted key to said second memory;

retrieving said encrypted data and said encrypted key from said second memory of said archive information system;

decrypting said encrypted data with said archive server encryption key;

transmitting said encrypted data and said encrypted key from said archive information system to said source information processing system;

decrypting said encrypted key with said master encryption key to recover said secondary key; and

decrypting said encrypted data with said secondary key to recover said data .

Generate Collection | Print

L2: Entry 1 of 3 File: USPT May 2, 2000

US-PAT-NO: 6058399
DOCUMENT-IDENTIFIER: US 6058399 A

TITLE: File upload synchronization

DATE-ISSUED: May 2, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Morag; Guy	Kohav Yair			IL
Samet; Yoav	Tel Aviv			IL
Entin; Leonid	Modi'in			IL
Rosenbaum; Yoni	Portola Vally	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
ColorDesk, Ltd.	Tel Aviv			IL	03

APPL-NO: 08/ 919862 [PALM]
DATE FILED: August 28, 1997

INT-CL: [07] G06 F 17/30

US-CL-ISSUED: 707/201; 707/202, 709/217, 709/203
US-CL-CURRENT: 707/201; 707/202, 709/203, 709/217

FIELD-OF-SEARCH: 707/201, 707/202, 707/203, 707/205, 709/217, 709/203, 348/7, 348/13, 710/113, 710/58, 710/61, 345/328

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5319455	June 1994	Hoarty et al.	348/7
☐	5392422	February 1995	Hoel et al.	710/113
☐	5721827	February 1998	Logan et al.	709/217
☐	5732216	March 1998	Logan et al.	709/203

ART-UNIT: 271

PRIMARY-EXAMINER: Amsbury; Wayne

ASSISTANT-EXAMINER: Havan; Thu-Thao

ATTY-AGENT-FIRM: Fenster & Company Patent Attorneys, Ltd.

ABSTRACT:

A method of synchronizing an interactive connection and a non-interactive data transfer connection between a client and a service provider, comprising:

creating an interactive connection;

creating a data transfer connection; and

generating a session ID which is associated with the two connections.

48 Claims, 5 Drawing figures

DOCUMENT-IDENTIFIER: US 6058399 A
TITLE: File upload synchronization

Application Filing Date (1):
19970828

Brief Summary Text (17):
A sixth aspect of some embodiments of the present invention is related to a process structure preferred for preferred embodiments of the invention Preferably, the service provider includes a WWW server, for the interactive session and an FTP server for the file upload session. Preferably, both servers are standard commercial software products, so that, preferably, they can be controlled externally, as black boxes. Preferably, each of the FTP server and the WWW server run on different machines. In a preferred embodiment of the invention, the service provider includes a synchronizing process which supplies the unique session ID and synchronizes the operation of the FTP server and the WWW server. Alternatively or additionally, the customer software may be provided with a synchronizing process. Alternatively or additionally, at least part of the synchronization is achieved from a third location. In a preferred embodiment of the invention, the customer software includes a standard WWW browser.

Detailed Description Text (22):
In a preferred embodiment of the invention, the step of receiving a unique session ID includes receiving a temporary user name and/or a password. Preferably, FTP client 12 uploads the image files, preferably to a unique location, using the provided user name and/or password. Additionally or alternatively, each uploaded file is associated with a unique session ID, preferably, by storing the file in a directory associated with the session ID or by appending the session ID to the name. In one preferred embodiment of the invention, the unique session ID is used to generate a unique user name and/or password. Alternatively, a bank of available user names may be used, from which a user name is cyclically selected. Thus, a user name will generally not be used simultaneously by two different customers. In some cases, especially when there are more active connections than user names, two customers will share a single user name. However, this should pose no problem, since files are still individually identified using their associated session IDs. Alternatively or additionally, the user name and/or the password are encrypted in the session ED, preferably using a public key encryption scheme. Thus, unique identification of the owner of the connection can be assured.

Generate Collection | Print

L2: Entry 2 of 3 File: USPT Aug 17, 1999

US-PAT-NO: 5940507
DOCUMENT-IDENTIFIER: US 5940507 A

TITLE: Secure file archive through encryption key management

DATE-ISSUED: August 17, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Cane; David	Sudbury	MA		
Hirschman; David	Sharon	MA		
Speare; Philip	Arlington	MA		
Vaitzblit; Lev	Concord	MA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Connected Corporation	Framingham	MA			02

APPL-NO: 09/ 014830 [PALM]
DATE FILED: January 28, 1998

PARENT-CASE:
CROSS REFERENCE TO RELATED APPLICATIONS A claim of priority is made to U.S. Provisional Patent Application No. 60/037,597, entitled FILE COMPARISON FOR DATA BACKUP AND FILE SYNCHRONIZATION, filed Feb. 11, 1997.

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/4; 380/21, 380/49
US-CL-CURRENT: 713/165; 380/277, 713/193

FIELD-OF-SEARCH: 380/4, 380/21, 380/49, 707/204, 711/161, 711/162, 395/186, 395/187.01, 713/200, 713/201

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE DATE	PATENTEE-NAME	US-CL
☐	5235641	August 1993	Nozawa et al.	380/21
☐	5416840	May 1995	Cane et al.	380/4
☐	5479654	December 1995	Squibb	395/600
☐	5559991	September 1996	Kanfi	395/489
☐	5584022	December 1996	Kikuchi et al.	380/21 X
☐	5719938	February 1998	Haas et al.	380/21
☐	5721777	February 1998	Blaze	380/4
☐	5748735	May 1998	Ganesan	380/21
☐	5764972	June 1998	Crouse et al.	395/601

OTHER PUBLICATIONS

Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd edition John Wiley and Sons, N.Y. (1995) p. 51 (Key and Message Transmission).

ART-UNIT: 276

PRIMARY-EXAMINER: Laufer; Pinchus M.

ATTY-AGENT-FIRM: Weingarten, Schurgin, Gagnebin & Hayes LLP

ABSTRACT:

A information processing system providing archive/backup support with privacy assurances by encrypting data stored thereby. Data generated on a source system is encrypted, the key used thereby is separately encrypted, and both the encrypted data and encrypted key are transmitted to and maintained by a data repository system. The repository system receives only the encrypted data and key, while the source system retains the ability to recover the key and in turn, the data. The source system is therefore assured of privacy and integrity of the archived data by retaining access control yet is relieved of the physical management of the warehousing medium.

24 Claims, 3 Drawing figures

Search Results - Record(s) 1 through 10 of 34 returned.

☐ 1. Document ID: US 20030105721 A1

L9: Entry 1 of 34 File: PGPB Jun 5, 2003

PGPUB-DOCUMENT-NUMBER: 20030105721
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030105721 A1

TITLE: Systems and methods for secure transaction management and electronic rights protection

PUBLICATION-DATE: June 5, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Ginter, Karl L.	Beltsville	MD	US	
Shear, Victor H.	Bethesda	MD	US	
Spahn, Francis J.	El Cerrito	CA	US	
Van Wie, David M.	Sunnyvale	CA	US	

US-CL-CURRENT: 705/54; 713/193

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

☐ 2. Document ID: US 20030088784 A1

L9: Entry 2 of 34 File: PGPB May 8, 2003

PGPUB-DOCUMENT-NUMBER: 20030088784
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030088784 A1

TITLE: Systems and methods for secure transaction management and electronic rights protection

PUBLICATION-DATE: May 8, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Ginter, Karl L.	Beltsville	MD	US	
Shear, Victor H.	Bethesda	MD	US	
Spahn, Francis J.	El Cerrito	CA	US	
Van Wie, David M.	Eugene	OR	US	

US-CL-CURRENT: 713/189; 713/182, 713/194

☐ 3. Document ID: US 20030084306 A1

L9: Entry 3 of 34 File: PGPB May 1, 2003

PGPUB-DOCUMENT-NUMBER: 20030084306
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030084306 A1

TITLE: Enforcement architecture and method for digital rights management system for roaming a license to a plurality of user devices

PUBLICATION-DATE: May 1, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Abburi, Rajasekhar	Medina	WA	US	
Alkove, James M.	Woodinville	WA	US	
McNeill, William P.	Seattle	WA	US	
McKune, Jeffrey R.	Issaquah	WA	US	

US-CL-CURRENT: 713/188; 705/59

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 4. Document ID: US 20030078853 A1

L9: Entry 4 of 34 File: PGPB Apr 24, 2003

PGPUB-DOCUMENT-NUMBER: 20030078853
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030078853 A1

TITLE: Enforcement architecture and method for digital rights management

PUBLICATION-DATE: April 24, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Peinado, Marcus	Bellevue	WA	US	
Abburi, Rajasekhar	Medina	WA	US	
Blinn, Arnold N.	Bellevue	WA	US	
Jones, Thomas C.	Redmond	WA	US	
Manferdelli, John L.	Redmond	WA	US	
Bell, Jeffrey R.C.	Seattle	WA	US	
Venkatesan, Ramaranthnam	Redmond	WA	US	
England, Paul	Bellevue	WA	US	
Jakubowski, Mariusz H.	Bellevue	WA	US	
Yu, Hai Ying (Vincent)	Bellevue	WA	US	

US-CL-CURRENT: 705/26

☐ 5. Document ID: US 20030028488 A1

L9: Entry 5 of 34 File: PGPB Feb 6, 2003

PGPUB-DOCUMENT-NUMBER: 20030028488
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030028488 A1

TITLE: Supervised license acquisition in a digital rights management system on a computing device

PUBLICATION-DATE: February 6, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Mohammed, Sohail Baig	North Bend	WA	US	
Olson, Kipley J.	Seattle	WA	US	
McKune, Jeffrey R.	Issaquah	WA	US	
Ganesan, Krishnamurthy	Redmond	WA	US	

US-CL-CURRENT: 705/59

☐ 6. Document ID: US 20030014655 A1

L9: Entry 6 of 34 File: PGPB Jan 16, 2003

PGPUB-DOCUMENT-NUMBER: 20030014655
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030014655 A1

TITLE: Protecting decrypted compressed content and decrypted decompressed content at a digital rights management client

PUBLICATION-DATE: January 16, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
England, Paul	Bellevue	WA	US	
Peinado, Marcus	Bellevue	WA	US	
Sankaranarayan, Mukund	Issaquah	WA	US	

US-CL-CURRENT: 713/200

☐ 7. Document ID: US 20020169974 A1

L9: Entry 7 of 34 File: PGPB Nov 14, 2002

PGPUB-DOCUMENT-NUMBER: 20020169974
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020169974 A1

TITLE: Detecting and responding to a clock rollback in a digital rights management system on a computing device

PUBLICATION-DATE: November 14, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
McKune, Jeffrey R.	Issaquah	WA	US	

US-CL-CURRENT: 713/200

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 8. Document ID: US 20020112171 A1

L9: Entry 8 of 34 File: PGPB Aug 15, 2002

PGPUB-DOCUMENT-NUMBER: 20020112171
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020112171 A1

TITLE: Systems and methods for secure transaction management and electronic rights protection

PUBLICATION-DATE: August 15, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Ginter, Karl L.	Beltsville	MD	US	
Shear, Victor H.	Bethesda	MD	US	
Spahn, Francis J.	El Cerrito	CA	US	
Van Wie, David M.	Eugene	OR	US	

US-CL-CURRENT: 713/185; 705/51, 713/200

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 9. Document ID: US 20020048369 A1

L9: Entry 9 of 34 File: PGPB Apr 25, 2002

PGPUB-DOCUMENT-NUMBER: 20020048369
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020048369 A1

TITLE: Systems and methods for secure transaction management and electronic rights protection

PUBLICATION-DATE: April 25, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Ginter, Karl L.	Beltsville	MD	US	
Shear, Victor H.	Bethesda	MD	US	
Sibert, W. Olin	Lexington	MA	US	
Spahn, Francis J.	El Cerrito	CA	US	
Van Wie, David M.	Eugene	OR	US	

US-CL-CURRENT: 380/277; 380/246, 713/151, 713/194

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 10. Document ID: US 20020019814 A1

L9: Entry 10 of 34 File: PGPB Feb 14, 2002

PGPUB-DOCUMENT-NUMBER: 20020019814
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020019814 A1

TITLE: Specifying rights in a digital rights license according to events

PUBLICATION-DATE: February 14, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Ganesan, Krishnamurthy	Redmond	WA	US	

US-CL-CURRENT: 705/59; 705/57, 707/10, 707/9

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

Generate Collection | Print

Terms	Documents
L8 and @pd>=19990327	34

Display Format: - Change Format

Previous Page Next Page

9/9 82,840

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 10 of 12 returned.

A ☐ 1. Document ID: US 6253193 B1

L6: Entry 1 of 12 File: USPT Jun 26, 2001

US-PAT-NO: 6253193
DOCUMENT-IDENTIFIER: US 6253193 B1
**** See image for Certificate of Correction ****

TITLE: Systems and methods for the secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

A ☐ 2. Document ID: US 6195432 B1

L6: Entry 2 of 12 File: USPT Feb 27, 2001

US-PAT-NO: 6195432
DOCUMENT-IDENTIFIER: US 6195432 B1

TITLE: Software distribution system and software utilization scheme for improving security and user convenience

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

A ☐ 3. Document ID: US 5982891 A

L6: Entry 3 of 12 File: USPT Nov 9, 1999

US-PAT-NO: 5982891
DOCUMENT-IDENTIFIER: US 5982891 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

A ☐ 4. Document ID: US 5949876 A

L6: Entry 4 of 12 File: USPT Sep 7, 1999

US-PAT-NO: 5949876
DOCUMENT-IDENTIFIER: US 5949876 A
**** See image for Certificate of Correction ****

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

A ☐ 5. Document ID: US 5917912 A

L6: Entry 5 of 12 File: USPT Jun 29, 1999

US-PAT-NO: 5917912
DOCUMENT-IDENTIFIER: US 5917912 A

TITLE: System and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

A ☐ 6. Document ID: US 5915019 A

L6: Entry 6 of 12 File: USPT Jun 22, 1999

US-PAT-NO: 5915019
DOCUMENT-IDENTIFIER: US 5915019 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

A ☐ 7. Document ID: US 5910987 A

L6: Entry 7 of 12 File: USPT Jun 8, 1999

US-PAT-NO: 5910987
DOCUMENT-IDENTIFIER: US 5910987 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

A ☐ 8. Document ID: US 5892900 A

L6: Entry 8 of 12 File: USPT Apr 6, 1999

US-PAT-NO: 5892900
DOCUMENT-IDENTIFIER: US 5892900 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

☐ 9. Document ID: US 5754649 A

L6: Entry 9 of 12 File: USPT May 19, 1998

US-PAT-NO: 5754649
DOCUMENT-IDENTIFIER: US 5754649 A

TITLE: Video media security and tracking system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

---

not obvious ☐ 10. Document ID: US 5754648 A

L6: Entry 10 of 12 File: USPT May 19, 1998

US-PAT-NO: 5754648
DOCUMENT-IDENTIFIER: US 5754648 A

TITLE: Video media security and tracking system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

Generate Collection | Print

Terms	Documents
L5 and rights	12

Display Format: TI Change Format

Previous Page Next Page

WEST

Generate Collection | Print

Search Results - Record(s) 11 through 12 of 12 returned.

non-obvious

☐ 11. Document ID: US 5513260 A

L6: Entry 11 of 12 File: USPT Apr 30, 1996

US-PAT-NO: 5513260
DOCUMENT-IDENTIFIER: US 5513260 A

TITLE: Method and apparatus for copy protection for various recording media

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

☐ 12. Document ID: US 4453074 A

L6: Entry 12 of 12 File: USPT Jun 5, 1984

US-PAT-NO: 4453074
DOCUMENT-IDENTIFIER: US 4453074 A

TITLE: Protection system for intelligent cards

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

Generate Collection | Print

Terms	Documents
L5 and rights	12

Display Format: TI Change Format

Previous Page Next Page

WEST

Your wildcard search against 10000 terms has yielded the results below.

Your result set for the last L# is incomplete.

The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

Generate Collection | Print

Search Results - Record(s) 1 through 5 of 5 returned.

Non-obvious

1. Document ID: US 5818934 A

L7: Entry 1 of 5 File: USPT Oct 6, 1998

US-PAT-NO: 5818934
DOCUMENT-IDENTIFIER: US 5818934 A

TITLE: Method and apparatus for providing a cryptographically secure interface between the decryption engine and the system decoder of a digital television receiver

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

2. Document ID: US 5754649 A

L7: Entry 2 of 5 File: USPT May 19, 1998

US-PAT-NO: 5754649
DOCUMENT-IDENTIFIER: US 5754649 A

TITLE: Video media security and tracking system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

3. Document ID: US 5754648 A

L7: Entry 3 of 5 File: USPT May 19, 1998

US-PAT-NO: 5754648
DOCUMENT-IDENTIFIER: US 5754648 A

TITLE: Video media security and tracking system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

☐ 4. Document ID: US 5513260 A

L7: Entry 4 of 5 File: USPT Apr 30, 1996

US-PAT-NO: 5513260
DOCUMENT-IDENTIFIER: US 5513260 A

TITLE: Method and apparatus for copy protection for various recording media

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

Non obvious

☐ 5. Document ID: US 4453074 A

L7: Entry 5 of 5 File: USPT Jun 5, 1984

US-PAT-NO: 4453074
DOCUMENT-IDENTIFIER: US 4453074 A

TITLE: Protection system for intelligent cards

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC
Draw Desc | Image

Generate Collection | Print

Terms	Documents
((black$ adj box$) same (encrypt$ or decrypt$)) and ((black$ adj box$) same ((private$ or public$) with key$)) and @pd<=19990327	5

Display Format: - Change Format

Previous Page Next Page

L7: Entry 1 of 5 File: USPT Oct 6, 1998

DOCUMENT-IDENTIFIER: US 5818934 A
TITLE: Method and apparatus for providing a cryptographically secure interface between the decryption engine and the system decoder of a digital television receiver

DATE ISSUED (1):
19981006

Brief Summary Text (4):
In public key encryption systems for digital television systems (and other types of digital data delivery systems), the decryption engine decrypts the encrypted television signal received by the digital television receiver in accordance with the corresponding decryption algorithm, using both a public key which depends upon the particular encryption algorithm employed, and a private key which is unknown and concealed within the decryption engine. The integrity of the security afforded by such systems depends upon preservation of the secrecy of the private key. If a pirate (attacker) is able to discover the private key, then it becomes a routine matter for the skilled pirate (an individual or company which has the capability to reverse engineer the decoder and decryption chips in the set-top box) to make other "bootleg" decryption chips and then incorporate them into "black boxes" that enable the reception of programming by a non-subscriber (i.e., a person who does not pay any subscription fees to the service provider).

Brief Summary Text (5):
In encryption systems for digital television systems (and other types of digital data delivery systems), there are two levels of encryption used public key encryption, and private key encryption. The bulk of the data is encrypted using a private key encryption (e.g. block ciphers like DES), owing to the speed of private key encryption. Sessions of the data transmission (typically, a session is several milliseconds of transmitted data) are encrypted with the block cipher using different private keys, called session keys; each session has its own private key. The session keys themselves are typically encrypted with a public key encryption system, wherein only the user holding the user private key of the public key system can decrypt, and thereby recover, the session key, which session key is used for decrypting the session of the transmitted data. The integrity of the security afforded by such a system depends mainly on the preservation of the secrecy of the user private key, and to a some extent on the secrecy of any one session key. If a pirate (attacker) is able to discover the user private key, then it becomes a routine matter for the skilled pirate (an individual or company which has the capability to reverse engineer the decoder and decryption chips in the set-top box, or digital data receiver) to make other "bootleg" decryption chips and then incorporate them into "black boxes" that enable the reception of programming by a non-subscriber (i.e., a person who does not pay any subscription fees to the service provider).

91

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 10 of 13 returned.

1. Document ID: US 6442525 B1

L6: Entry 1 of 13 File: USPT Aug 27, 2002

US-PAT-NO: 6442525
DOCUMENT-IDENTIFIER: US 6442525 B1

TITLE: System for authenticating physical objects

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

2. Document ID: US 6397333 B1

L6: Entry 2 of 13 File: USPT May 28, 2002

US-PAT-NO: 6397333
DOCUMENT-IDENTIFIER: US 6397333 B1

TITLE: Copy protection system and method

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

3. Document ID: US 6343280 B1

L6: Entry 3 of 13 File: USPT Jan 29, 2002

US-PAT-NO: 6343280
DOCUMENT-IDENTIFIER: US 6343280 B1

TITLE: Distributed execution software license server

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. Desc | Image

4. Document ID: US 6253193 B1

L6: Entry 4 of 13 File: USPT Jun 26, 2001

US-PAT-NO: 6253193
DOCUMENT-IDENTIFIER: US 6253193 B1
**** See image for Certificate of Correction ****

TITLE: Systems and methods for the secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Image

---

5. Document ID: US 6134536 A

L6: Entry 5 of 13 File: USPT Oct 17, 2000

US-PAT-NO: 6134536
DOCUMENT-IDENTIFIER: US 6134536 A
**** See image for Certificate of Correction ****

TITLE: Methods and apparatus relating to the formulation and trading of risk management contracts

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Image

---

6. Document ID: US 6021202 A

L6: Entry 6 of 13 File: USPT Feb 1, 2000

US-PAT-NO: 6021202
DOCUMENT-IDENTIFIER: US 6021202 A

TITLE: Method and system for processing electronic documents

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Image

---

7. Document ID: US 6018712 A

L6: Entry 7 of 13 File: USPT Jan 25, 2000

US-PAT-NO: 6018712
DOCUMENT-IDENTIFIER: US 6018712 A

TITLE: Method and apparatus for remote program execution to use in computer software protection without the use of encryption

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

8. Document ID: US 5982891 A

L6: Entry 8 of 13 File: USPT Nov 9, 1999

US-PAT-NO: 5982891
DOCUMENT-IDENTIFIER: US 5982891 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 9. Document ID: US 5949876 A

L6: Entry 9 of 13 File: USPT Sep 7, 1999

US-PAT-NO: 5949876
DOCUMENT-IDENTIFIER: US 5949876 A
**** See image for Certificate of Correction ****

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 10. Document ID: US 5915019 A

L6: Entry 10 of 13 File: USPT Jun 22, 1999

US-PAT-NO: 5915019
DOCUMENT-IDENTIFIER: US 5915019 A

TITLE: Systems and methods for secure transaction management and electronic rights protection

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

Generate Collection | Print

Terms	Documents
L5 and (decrypt$ or encrypt$)	13

Display Format: TI Change Format

WEST

Generate Collection | Print

Search Results - Record(s) 11 through 13 of 13 returned.

☐ 11. Document ID: US 5754649 A

L6: Entry 11 of 13 File: USPT May 19, 1998

US-PAT-NO: 5754649
DOCUMENT-IDENTIFIER: US 5754649 A

TITLE: Video media security and tracking system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw. Desc | Image

☐ 12. Document ID: US 5754648 A

L6: Entry 12 of 13 File: USPT May 19, 1998

US-PAT-NO: 5754648
DOCUMENT-IDENTIFIER: US 5754648 A

TITLE: Video media security and tracking system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw. Desc | Image

☐ 13. Document ID: US 5109413 A

L6: Entry 13 of 13 File: USPT Apr 28, 1992

US-PAT-NO: 5109413
DOCUMENT-IDENTIFIER: US 5109413 A
**** See image for Certificate of Correction ****

TITLE: Manipulating rights-to-execute in connection with a software copy protection mechanism

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw. Desc | Image

Generate Collection | Print

Terms	Documents
L5 and (decrypt$ or encrypt$)	13

Display Format: TI Change Format

Previous Page Next Page